DRAFT

AMENDMENTS to the CLAIMS

The following listing of claims highlight changes between the last set of amended claims, as relied upon in the Office Action dated May 20, 2004, and the newly amended claims. These newly amended claims will replace all prior versions, and listings, of claims in the application:

Listing of the Claims

Claim 79 (currently amended): A system for transfer of secure data on a network comprising:

a) a client capable of presenting conforming client data;

b) a server capable of using said conforming client data to create at least ~~one~~ two secure cookie, each of said at least one secure cookie including:

i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid;

ii) at least one name field capable of holding name data;

iii) at least one value field capable of holding value data derived from said conforming client data; and

iv) an expiration field capable of holding cookie expiration data;

c) a network capable of transporting at least one of said at least ~~one~~ two secure cookie between said server and said client;

d) a client storage means capable of storing at least one of said at least one secure cookie; and

e) a secure attribute service between said client and said server using said at least one of said at least one secure cookie,

wherein at least one of said at least ~~one~~ two secure cookie is ~~one of the following:~~

~~a) an authentication cookie;~~

~~b) a seal cookie, capable of being used by said server to determine if at least one of said at least one secure cookie has been altered; and~~

~~c)~~ a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least one secure cookie.

Claim 80 (previously added): A system according to claim 79, wherein said client is a web browser.

Claim 81 (canceled)

Claim 82 (previously added): A system according to claim 79, wherein said secure attribute service includes said server authenticating said client by comparing said conforming client data with said value data.

Claim 83 (currently amended): A system according to claim [[79]] 119, wherein said authentication cookie is an IP cookie and said conforming client data includes the IP address of said client.

DRAFT

Claim 84 (currently amended): A system according to claim [[79]] 119, wherein said authentication cookie is a password cookie and said conforming client data includes a password.

Claim 85 (previously added): A system according to claim 84, wherein said password is processed using a hashing algorithm.

Claim 86 (previously added): A system according to claim 84, wherein said password is processed using an encryption algorithm.

Claim 87 (currently amended): A system according to claim [[79]] 119, wherein said authentication cookie is a sign cookie and said conforming client data includes a digital signature on a timestamp.

Claim 88 (currently amended): A system according to claim [[79]] 119, further including a secret-key based authentication service.

Claim 89 (previously added): A system according to claim 88, and wherein said authentication cookie is a KT cookie and said conforming client data includes a Kerberos ticket created using a Kerberos protocol.

Claim 90 (previously added): A system according to claim 79, wherein at least one of said at least one secure cookie includes a multitude of secure cookies.

Claim 91 (canceled)

Claim 92 (currently amended): A system according to claim [[79]] 118, wherein said seal cookie includes an integrity check value.

Claim 93 (currently amended): A system according to claim [[79]] 118, wherein said seal cookie includes the signature of a message digest signed using a private key.

Claim 94 (previously added): A system according to claim 79, wherein at least one of said at least one name field and at least one of said at least one value field are a pair.

Claim 95 (previously added): A system according to claim 79, wherein at least one of said at least one secure cookie further includes a flag, said flag specifying whether all machines within said domain referenced by said domain data can access said value data.

Claim 96 (canceled)

Claim 97 (previously added): A system according to claim 79, wherein at least one of said at least one secure cookie is used in an electronic transaction.

DRAFT

Claim 98 (previously added): A system according to claim 79, wherein said system is part of a role based access control system and at least one of said at least one secure cookie is used in assigning client roles.

Claim 99 (currently amended): A method for the transfer of secure data on a network including the steps of:

a) a client making a request from a server;
b) said server retrieving conforming client data;
c) said server creating at least one secure cookie, each of said at least one secure cookie including selected conforming client data, said selected conforming data including at least some of said conforming client data;
d) said server transmitting at least one of said at least one secure cookie to said client;
e) said client storing at least one of said at least one secure cookie;
f) said client presenting to a related server at least one of said stored at least one secure cookie with a second request, said related server residing on the same domain as said server;
g) said related server making a determination of whether at least one of said at least one retrieved stored at least one secure cookie contains said selected conforming client data; and
h) said related server fulfilling said second request if said determination is positive[[,]];

wherein at least one of said at least one secure cookie is ~~one of the following:~~

~~a) an authentication cookie;~~
~~b) a seal cookie, capable of being used by said server to determine if at least one of said at least one secure cookie has been altered; and~~
~~c)~~ a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least one secure cookie.

Claim 100 (previously added): A method of claim 99 wherein at least some of said conforming client data is retrieved from said client.

Claim 101 (previously added): A method of claim 99, wherein said conforming client data includes a client's IP address.

Claim 102 (previously added): A method of claim 99, wherein said conforming client data includes a password.

Claim 103 (previously added): A method of claim 99, wherein said conforming client data includes a Kerberos ticket.

Claim 104 (previously added): A method of claim 99, wherein said conforming client data includes a digital signature.

DRAFT

Claim 105 (previously added): A method of claim 104, wherein said determination further includes verifying that said digital signature belongs to said client.

Claim 106 (previously added): A method of claim 99, further including the step of said server encrypting at least some of said selected conforming client data.

Claim 107 (previously added): A method of claim 106, wherein said encrypting uses a public key.

Claim 108 (previously added): A method of claim 106, wherein said encrypting uses a secret key.

Claim 109 (previously added): A method of claim 106, further including the step of said server decrypting said encrypted selected conforming client data using a private key.

Claim 110 (previously added): A method of claim 106, further including the step of said server decrypting said encrypted selected conforming client data using a secret key.

Claim 111 (previously added): A method of claim 99, further including the step of said server hashing at least some of said conforming client data.

Claim 112 (previously added): A method of claim 99, wherein said conforming client data includes data derived from at least one item from the group consisting of:

a) the client's IP address;
b) a password;
c) a Kerberos ticket;
d) credit card data;
e) social security number;
f) a digital signature of the client; and
g) a home address.

Claim 113 (previously added): A method of claim 99, wherein said determination is positive only if said selected conforming client data was retrieved by said server from said client during the current session.

Claim 114 (previously added): A method of claim 99, wherein said secure cookie contains a digital signature of said client on a time-stamp.

Claim 115 (previously added): A method of claim 99, further including the step of providing integrity to at least one of said at least one secure cookie comprising:

a) said server creating integrity data from at least one of said at least one secure cookie, said integrity data including at least one item selected from the group:
   i) encrypted said selected conforming client data;
   ii) a digital signature; and

DRAFT

iii) a message digest;
b) said server inputting said integrity data into a seal cookie; and
c) said server storing said seal cookie.

Claim 116 (previously added): A method of claim 99, wherein said request is part of an electronic transaction.

Claim 117 (previously added): A method of claim 99, wherein said request is part of an attribute-based access control function.

Claim 118 (new): A system for transfer of secure data on a network comprising:
a) a client capable of presenting conforming client data;
b) a server capable of using said conforming client data to create at least one secure cookie, each of said at least one secure cookie including:
i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid;
ii) at least one name field capable of holding name data;
iii) at least one value field capable of holding value data derived from said conforming client data; and
iv) an expiration field capable of holding cookie expiration data;
c) a network capable of transporting at least one of said at least one secure cookie between said server and said client;
d) a client storage means capable of storing at least one of said at least one secure cookie; and
e) a secure attribute service between said client and said server using said at least one of said at least one secure cookie; and
wherein at least one of said at least one secure cookie is a seal cookie, capable of being used by said server to determine if at least one of said at least one secure cookie has been altered.

Claim 119 (new): A system according to claim 79, wherein at least one of said at least one secure cookie is an authentication cookie.

Claim 120 (new): A method for the transfer of secure data on a network including the steps of:
a) a client making a request from a server;
b) said server retrieving conforming client data;
c) said server creating at least one secure cookie, each of said at least one secure cookie including selected conforming client data, said selected conforming data including at least some of said conforming client data;
d) said server transmitting at least one of said at least one secure cookie to said client;
e) said client storing at least one of said at least one secure cookie;
f) said client presenting to a related server at least one of said stored at least one secure cookie with a second request, said related server residing on the same domain as said server;

DRAFT

g) said related server making a determination of whether at least one of said at least one retrieved stored at least one secure cookie contains said selected conforming client data; and

h) said related server fulfilling said second request if said determination is positive;

wherein at least one of said at least one secure cookie is a seal cookie, capable of being used by said server to determine if at least one of said at least one secure cookie has been altered.

Claim 121 (new): A method according to claim 99, wherein at least one of said at least one secure cookie is an authentication cookie.